

Army
PHIMT Training: Service Specific and Policy Related
Questions and Answers

- 1. Q: Do we still have to maintain a paper trail as we have been doing?**
A: TMA Privacy Office has not yet released any guidance relating to retaining paper documents; please remain in compliance with this to the Army's requirements. *Army Note: The paper trail to the patient's record and to the facility's files is still required.*
- 2. Q: Is there additional personnel that will be put into place to support this new application?**
A: The application is provided as a tool for existing personnel to use in order to comply with HIPAA Privacy Rule, mainly, for tracking and accounting for disclosures. It is not expected that additional personnel will be needed to support the application. However, individual MTFs may determine otherwise.
- 3. Q: Who determines the cost of providing copies of records or an accounting of disclosures to an individual?**
A: Please refer this to your Service's policies. You have the option as whether or not you are going to charge them. This requirement is set at a local or Service level.
- 4. Q: Who determines the cost for recording a request?**
A: The cost for recording a request will vary from one site to another, depending upon the workflow. The cost is zero for the MTF, and the service, as they will not be storing and maintaining the database. Of course there is a learning curve for the transition of whatever procedure is currently in place and the one required for using the PHIMT. Additionally, until the application can auto populate patient demographics (either by way of previous records manually created, or by way of some systemic resolution,) then there is a minimal cost of time spent by the user to input that information.
- 5. Q: When is the required "Go Live" date?**
A: The User Admins have been granted access to the PHIMT and will set up additional user accounts for access. Your Service Representative will determine a "Go Live" date. MHS has not yet declared a date for mandatory usage of PHIMT; however, it is imperative that each facility has a way to provide a record of disclosures upon request from the patient.
- 6. Q: Can we transfer the data in the current application that is being used into PHIMT?**
A: We have provided the Service Representatives with the necessary mapping information. The mapping document should be attached to this communication.

Army
PHIMT Training: Service Specific and Policy Related
Questions and Answers

7. **Q: Can you give an example of a service user admin?**
A: This would be a user at the Army level instead of at a local MTF.
8. **Q: Does the tool have a billing feature which would allow our MTF to bill attorney's offices and other clients?**
A: PHIMT does not currently include any billing features. MTFs should continue using the billing process currently in use at their facility. The billing feature will be utilized upon Phase II deployment.
9. **Q: I am a pharmacist, and am wondering whether information about patient pick-ups of their own prescriptions needs to be entered into the tool. In other words, does a disclosure of PHI via prescription requests and sick slips need to be entered into PHIMT?**
A: When patients picking up their prescriptions provide self-identification this is not considered a disclosure and so does not need to be entered into PHIMT. However, in cases where PHI is not being transmitted directly to the patient, as when profiles are being sent, TMA suggests that this transmittal should be tracked using the tool. In short, if a patient signs for their own information, it is not a disclosure and does not need to be tracked. Protocol for dealing with PHI contained in profiles is being developed at the service level.
10. **Q: Is there a filter that allows users to remove disclosures entered before an authorization is granted? The MTF is not required by law to provide disclosures pursuant to authorizations granted. Is there a filter to remove such disclosures?**
A: This question assumes that granting an authorization for a time period **prior** to that authorization date is permissible. If a disclosure record is created, then it is reported, unless suspended. Therefore, if a disclosure record is created when an authorization is on file, then it cannot be removed from the database. TMA only requires disclosures to be tracked; the authorization module is optional and its use will vary by service-specific requirements. To generate a record of authorizations only, omitting prior disclosures, users may select the "authorizations" from the screen listing all disclosure types.
11. **Q: Who at my MTF should receive a password to the tool? I have not yet received a password.**
A: The password should be given to the User Administrator, as designated by your Service Representative, prior to deployment and training. The Privacy Officer is then responsible for determining the individuals who will have access and the User Admin is responsible for verifying identity and distributing passwords.

Army
PHIMT Training: Service Specific and Policy Related
Questions and Answers

12. Q: Why is AR 40-66 (pertaining to billing) not incorporated into PHIMT?

A: Billing functionality is not yet included in this tool. MTFs should continue use of their current billing practices.

13. Q: On the LMS, we had the ability to transfer...so you can't do this with the tool? Why?

A: It is a separate COTS product, having no connection whatsoever to the LMS product. It is necessary to associate a user with a particular MTF at any given time, in order for auditing to take place. Collaboration between the service-level User Admin and the Privacy Officers must take place in order for a user to be given access at a different MTF. A "transfer" within the PHIMT assumes that the user will have the same access privileges at the next facility, when that may not be the case.

14. Q: In using this system, are we able to see the patients for the other services?

A: Yes, you will be able to see the patients across the MHS.

15. Q: Are we responsible for making sure that the outside clinics/subordinates get on board and get trained?

A: Yes. The Privacy Officer at a MTF with subordinate clinics is responsible for all users getting training and access to the PHIMT.

Accessing PHIMT:

1. Q: How do I access the PHIMT?

A: You access the PHIMT through the URL - <https://phimt.tricare.osd.mil>

Password:

2. Q: Is it necessary to always create a new password or will unlocking the account enable the old password?

A: No. Unlocking the account will enable the old password. The reason for unlocking the account or resetting the password is because the user does not remember their password.

3. Q: Is there a need to change passwords on a frequent basis?

A: Yes, you will be required to change your password every 90 days.

4. Q: Is there a password history?

A: Yes, the system remembers 24 passwords in the history.

Army
PHIMT Training: Service Specific and Policy Related
Questions and Answers

5. **Q: Do passwords require special characters?**
A: Yes, passwords must be 6-15 characters long and contain an upper case letter, lower case letter, a number, and a symbol.
6. **Q: For those in the clinics, are you going to send out the passwords for the PHIMT?**
A: Yes, we will provide the User Admins with their login information, the User Admins will then add additional Users within their facility and distribute their login information as necessary.

Users and User Roles:

7. **Q: Who will assign the initial account information for the User Admin?**
A: The HIPAA Support Center will assign the initial account information and send the login information to the respective User Admins.
8. **Q: Can the User Admin delete users or should they deactivate the account?**
A: No, the User Admins cannot delete users. They should deactivate the account by placing a check in the "User Disabled" checkbox located on the User Profile screen.
9. **Q: How many Users can a facility have?**
A: A facility can have as many Users as they would like to assign. Typically these will be individuals within the Medical Records department or other departments that release patient data.
10. **Q: Will there be more than one Privacy Specialist at each facility?**
A: You can set up as many designees as you wish. They do not have to be the Privacy Officer, but it is up to the discretion of the Privacy Officer or individual MTF policy.
11. **Q: Can User Admins add as many Regular Users as they need?**
A: Yes, there is no limit of how many Regular Users a facility can have; however you should follow your facilities procedures.
12. **Q: Can a User have more than 2 roles?**
A: Yes, a User could have multiple roles; for example, one could be a User Admin, Regular User and Privacy Specialist.
13. **Q: What should be done if a User transfers from one MTF to another?**
A: The User is deactivated at one MTF and reactivated at another MTF, by the User Admin at the Service level.

Army
PHIMT Training: Service Specific and Policy Related
Questions and Answers

14. Q: Do you need certain User roles to access certain screens?

A: Yes, selecting the appropriate role allows you to access data within certain screens. When a User logs into the application they will only be able to view the tabs in which they have access to.

15. Q: How many Administrators can you have?

A: That is up to the Privacy Officer to decide how many administrators they need. The number is not limited.

16. Q: What do we do with our remote clinics that need access?

A: You give User rights to whoever needs to have access at your clinic(s) whether or not it is remote. You can train them through the presentations and the course catalog found on the LMS at www.hipaatraining.tricare.osd.mil.

17. Q: If employees will be releasing the information, should they be set up as a Regular User or a Privacy Officer?

A: If they will be approving/denying the disclosures, they have to have the Privacy Specialist role. It is up to the MTF to decide who has what role and then how many people to assign these roles.

18. Q: What do you do when an individual changes their status from military to civilian or even to contractor?

A: If they are still going to be working for the same MTF they can keep their access to the system. If they are leaving the MTF, they will need to be disabled and added as a User at their new facility.

Searches:

19. Q: Are the search fields case sensitive?

A: No, the search fields are not case sensitive.

20. Q: One of the first steps is a search. Are all patients already in the database, or will we be entering new names when not found.

A: You will be entering the patients into the application.

21. Q: When I perform a query on a patient, will I have access to all patients across the country?

A: Yes, you will have access to all patients that have been entered in the system.

Army
PHIMT Training: Service Specific and Policy Related
Questions and Answers

22. Q: Can you search for a patient by SSN or the Sponsor's SSN?

A: You can search by last name. If multiple last names exist, then you will be able to view the SSN's for those people and select the appropriate one.

23. Q: Will you be able to leave fields blank in PHIMT?

A: Only information that isn't required can be left blank. If you leave a required field blank, you will get an error message upon saving or updating the information.

Patients

24. Q: Can patients request a copy of their complete outpatient record orally?

A: Yes, a patient can request a copy of their complete outpatient records orally. There is a field within the Request tab in which you can select indicating that record was requested orally.

25. Q: How do you handle the record for a former Active Duty member who then becomes a dependent? Do you maintain two records or change the name and SSN on the Active Duty record?

A: The Active Duty member that becomes a dependant may still be maintained within the PHIMT as a separate record. The system has the flexibility to allow the changing of a name and/or a SSN and maintain the original record. As in other systems (CHCS), you are not required to generate a new record within the system if your status changes.

26. Q: If a patient transfers, how is access to the patient's data affected?

A: If a patient transfers, access to their data is not affected. Patient access is global; therefore no transfer is required. You will have access to all patients that are entered within your Service.

Authorizations

27. Q: Do the authorization forms generated by PHIMT meet current legal standards?

A: Yes, these forms meet current legal standards and have been reviewed by legal experts at the Service and Department of Defense levels.

28. Q: If an authorization were to be granted/denied accidentally, would there be a way to recall that authorization?

A: This can be done in the system by revoking the authorization.

Army
PHIMT Training: Service Specific and Policy Related
Questions and Answers

29. Q: If there is an authorization in the medical record to release the record to a spouse, do you have to account for each subsequent disclosure in the disclosure-tracking tool?

A: Yes, any accountable disclosure needs to be tracked in the tool.

30. Q: Since the PHIMT tool records authorizations electronically, is it still necessary to keep a hard copy? Where should the hard copy of the authorization be kept?

A: Hard copies of authorizations should always be maintained, even if authorizations are recorded electronically. These copies should be stored in a convenient location. However, the specific storage location remains at the discretion of the MTF and/or health plan.

Letters

31. Q: Will the letters be generated locally or at TMA?

A: Letters are generated locally.

32. Q: Will the tool create a "suspension letter"?

A: Yes, it will create a "suspension letter".

33. Q: Are letters generated in PHIMT tailored to individual MTFs?

A: All letters generated in PHIMT are automatically tailored to the MTF where they are produced. Each letter bears the appropriate Army, Navy, or Air Force seal. It also displays the individual MTFs mailing address and supplementary contact information.

34. Q: PHIMT generates its letters as PDFs, making it difficult to add additional information, such as why a disclosure request was denied. Could this be changed?

A: Not at this time, but this is an excellent concern and will be passed to the technical team for consideration and addition during Phase II.

Miscellaneous:

35. Q: What is office workflow?

A: Office workflow is considered the business process by which you identify the approval process or designees for approving or denying the request of PHI disclosures.

Army
PHIMT Training: Service Specific and Policy Related
Questions and Answers

36. Q: Will the alternate communication request by the patient be mandatory or an optional feature?

A: This is an optional feature.

37. Q: Will PHIMT be able to support the longer European phone numbers?

A: The system does not currently support European phone numbers, but we will look into incorporating this feature in the next phase.

38. Q: Will the system allow for the disclosure request status? Example: Draft, complete etc.?

A: Yes, it will show whether the disclosure is pending or approved.

39. Q: Does the Disclosure Request save when you select "Pending" for the status?

A: Yes, the Disclosure Request will be saved and you will be able to go back into the request and update it with the appropriate status. All fields on the record are writable/changeable while the disclosure is in a Pending status.

40. Q: Once a disclosure has been saved, can you go back and edit the details?

A: You can create an amendment to the Disclosure by entering text into the comments field and selecting Update for that disclosure.

41. Q: If the Disclosure Type that you want to select is not in the drop down list, can you enter free text into the field?

A: You cannot enter free text into the Disclosure Type field. However, you can select "Other" from the drop down list and enter additional information into the comments field.

42. Q: Can you print out all of the Disclosures for a patient?

A: Yes, you can generate a form through the Requests tab that will provide you with an Accounting of Disclosures for a given patient. This report does not include any disclosures that have been suspended.

43. Q: Will future functionality allow you to merge two records?

A: Currently the system does not allow a User to merge two records. This functionality can certainly be considered for future enhancements.

44. Q: Is the server reliable? Is there a backup plan if there are technological problems? If a problem does arise, should we resort back to the old way of doing things?

Army
PHIMT Training: Service Specific and Policy Related
Questions and Answers

A: The PHIMT is on a secure server; it is on a government server with government furnished equipment and in a secure location that meets all the security requirements. We do have a disaster recovery plan in place. If there is a technological problem, we will send out a notification of when and how long the system will be down.

45. Q: What is the HIPAA Support Center's response time for answering any questions?

A: The HIPAA Support Center's response time is a three business days.

46. Q: The PHIMT tool prompts Users to enter both a start date and an end date for disclosure restrictions. Is there a reminder feature in the system that tells users that an end date is approaching?

A: Although this feature is not currently available, upgrades are being made to the tool based on user feedback and such a feature could certainly be added. Additional suggestions for ways to improve the tool are also encouraged.

47. Q: Where can users record additional information about the release of PHI, such as why and to whom the information was made available?

A: When needed, this information can be recorded in the Comments field.

48. Q: We would like to streamline the data entry process at my MTF. We would like to record PHI information quickly and as non-electronically as necessary and later enter this data into PHIMT. Is this possible?

A: Yes, there are various ways to enter patient information into PHIMT. Choose the process which best meets your operational needs and abilities.

49. Q: Can PHIMT generate mailing labels or other kinds of labels?

A: PHIMT does not currently possess this capability; however, this is a feature that will be considered for additional updates.

50. Q: Other, similar tools allow MTFs to track requests (in addition to disclosures and authorizations), although PHIMT does not currently possess this capability. Might this functionality be included in future versions of the tool?

A: The ability to track requests is being considered for addition to future versions of the PHIMT and will be included in Phase II.

Army
PHIMT Training: Service Specific and Policy Related
Questions and Answers

51. Q: Will users have the opportunity to experiment with the tool to familiarize themselves, hands-on, before the tool goes into use?

A: Since moving between screens requires that patient data be saved, there is not currently a method that allows users to experiment with the tool without entering actual patient data.

52. Q: With regard to the security features of the tool itself, does this tool have a “distant shutdown” or “timeout” feature that would close a session after x minutes without use?

A: Yes, the tool does have a timeout feature that ends sessions following a period of non-use. The tool is currently in the process of becoming DITSCAP certified and this feature is one of many which will ensure the security of the system.

53. Q: On the Registration page under User profile, do you have to have a .mil address?

A: No, a .mil address is not required for this system. However, it is recommended that you use your .mil address.

54. Q: Do you have to have a password to access the course catalog?

A: The course catalog is not located on the PHIMT, but rather on the LMS. You should use your Student ID and password to access the posted courses on the LMS under the course catalog at www.hipaatraining.tricare.osd.mil.

For additional questions related to the PHIMT please contact the HIPAA Support Center at: hipaasupport@tma.osd.mil.